ManageEngine

Navigating the **Digital Personal Data Protection** Act:

A comprehensive guide for compliance with ManageEngine solutions

Table of contents

Introduction to the Digital Personal Data Protection Act, 2023

Summary

The Digital Personal Data Protection (DPDP) Act, 2023 marks India's formal entry into the global landscape of modern data governance. Unlike previous regulations, it shifts the focus from mere compliance to accountability, placing clear obligations on businesses while empowering individuals with enforceable rights over their digital footprint. Understanding and adhering to the DPDP Act is crucial for all entities that handle personal data within India or process the data of Indian citizens, regardless of their geographical location.

This e-book provides an in-depth analysis of the DPDP Act, explains its key requirements, and explores how ManageEngine AD360 and Log360 can assist organizations in meeting their compliance obligations. By leveraging AD360 and Log360, businesses can enhance their data protection posture, streamline compliance efforts, and build trust with their stakeholders.

Why a data protection act is needed in India

With the rapid growth of digital technologies and online services, the collection and processing of personal data has become increasingly prevalent. Prior to the DPDP Act, India lacked a comprehensive privacy law. While the Supreme Court of India recognized the right to privacy as a constitutionally protected right in 2017, the existing Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules) had limitations.

The DPDP Act aims to fill this crucial gap by providing a comprehensive legal framework for data protection in India. Furthermore, there was a lack of clarity regarding individuals' legal rights regarding their personal data and a lack of accountability for organizations processing this data. The DPDP Act establishes the Data Protection Board of India (DPB) to enforce the law and hold organizations accountable, thereby empowering individuals with greater control over their personal data.

Overview of the DPDP Act and its objectives

The DPDP Act is aims to establish a robust framework for data protection, ensuring accountability, transparency, and consent-based data handling practices across various sectors. It establishes a balance between the need for lawful data processing and an individual's right to safeguard their personal data.
Under this law, entities handling personal data (referred to as Data Fiduciaries) are assigned specific responsibilities to ensure proper data management. At the same time, individuals whose data is being processed (known as Data Principals) are granted defined rights and obligations to maintain control over their personal information. Additionally, it enforces accountability by imposing monetary penalties on organizations that violate its regulations.

Brief history of data privacy laws in India

Prior to 2023, India did not have a standalone law on data protection; the use of personal data was regulated under the Information Technology (IT) Act, 2000 and the SPDI Rules.

In 2017, the Supreme Court of India's Puttaswamy judgment recognized the right to privacy as a fundamental right. Following this, the government developed draft legislation to protect the privacy of Indians. This included the Personal Data Protection Bill, 2019, which was based on the recommendations of a Committee of Experts on Data Protection chaired by Justice B. N. Srikrishna. This bill was referred to a Joint Parliamentary Committee but was eventually withdrawn in August 2022.

Subsequently, the Ministry of Electronics and Information Technology proposed the Digital Personal Data Protection Bill, 2022 in November 2022. After further deliberation and amendments, the Digital Personal Data Protection Act, 2023 was passed by the Indian Parliament in August 2023 and received presidential assent.

Status, applicability, and scope of the DPDP Act

The DPDP Act applies to the processing of digital personal data within India where the data is collected online or offline and is subsequently digitized. It also has extraterritorial application, extending to the processing of digital personal data outside of India if such processing is related to offering goods or services to individuals within India. This means organizations based outside India but targeting the Indian market will also need to comply with the DPDP Act.

Exclusions from the DPDP Act

While the scope of the DPDP Act is broad, it also outlines certain exclusions. It does not apply to personal data processed for personal or domestic purposes by individuals. It also excludes non-automated personal data, meaning data processed manually and not digitized, as well as offline personal data that remains in physical form and is not converted into a digital format. Personal data that has been made publicly available by the Data Principal themselves or by any other person under a legal obligation to do so is also generally outside the purview of the Act. Additionally, data processed for law enforcement or national security purposes may be exempt. Data processed for journalistic or artistic expression is also exempt. Understanding these exclusions is crucial for organizations to accurately determine which of their data processing activities are governed by the DPDP Act.

Demystifying the DPDP Act, 2023

Key principles and definitions

A. Key principles of the DPDP Act

The DPDP Act is built upon six fundamental principles that serve as guidelines for the lawful processing of personal data. These principles provide the ethical and legal foundation of the Act.

Key principles	Explanation
Lawfulness	This principle dictates that personal data must be processed in a manner that is **lawful, fair,** and **transparent to the individuals concerned**. This implies that processing must have a legal basis, be conducted in good faith, and provide individuals with clear information about how their data is being handled.
Purpose limitation	This principle mandates that personal data should be collected for **specified, explicit,** and **legitimate purposes** and **not further processed in a way incompatible with those original purposes**. This means that organizations must clearly define why they are collecting personal data and can only use it for those stated reasons, unless a new purpose is compatible with the original purpose.
Data minimization	This principle emphasizes that personal data must be **adequate, relevant,** and **limited to what is necessary for the purposes for which it is processed**. Organizations should only collect and retain the personal data that is strictly required to fulfill the specified purposes.
Accuracy	This principle requires that **personal data is accurate** and **kept up to date where necessary.** Data Fiduciaries have an obligation to make reasonable efforts to ensure the accuracy and completeness of personal data.
Storage limitation	This principle stipulates that **personal data should be retained only as long as necessary to fulfill the purposes for which it was processed.** Data Fiduciaries must erase personal data when the Data Principal withdraws consent or when it is reasonable to assume the specified purpose is no longer being served, unless retention is necessary for compliance with any law. For government entities, storage limitation may not always apply.
Integrity and confidentiality	This principle necessitates that **personal data is processed in a manner that ensures appropriate security, protecting against unauthorized or unlawful processing, accidental loss, destruction, or damage through suitable technical and organizational measures.** Data Fiduciaries are responsible for implementing reasonable security safeguards to prevent personal data breaches.

B. Key definitions of the DPDP Act

A clear understanding of the DPDP Act's key definitions is essential for effectively navigating and complying with its provisions.

Entity	Definition
Personal data	This is defined as **any data about an individual who can be identified by or in relation to such data.** This is a broad definition encompassing a wide range of information, including name, address, contact details, date of birth, financial information, online browsing history, social media posts, and location data. The Act also considers indirectly identifiable information such as vehicle numbers and employee codes as personal data.
Digital personal data	This refers to **personal data that is in digital form, irrespective of whether it was initially collected digitally or in non-digital form and subsequently digitized.** The Act's scope is primarily focused on digital personal data.
Processing	This includes **any operation performed on digital personal data, whether wholly or partly automated, such as collection, recording, organization, structuring, storage, adaptation, retrieval, use, sharing, and erasure.** This definition covers the entire life cycle of digital personal data.
Data Principal	This is the **individual to whom the personal data relates.** This includes parents or lawful guardians acting on behalf of children or persons with disabilities. The DPDP Act grants several rights to Data Principals concerning their personal data.
Data Fiduciary	This is **any person who, alone or in conjunction with others, determines the purpose and means of processing personal data.** Data Fiduciaries bear the primary responsibility for compliance with the DPDP. They have several obligations, such as providing notice, obtaining consent, ensuring data accuracy and security, and reporting data breaches. Certain Data Fiduciaries may be designated as Significant Data Fiduciaries (SDF), incurring additional obligations.
Significant Data Fiduciary (SDF)	These are Data Fiduciaries that may be **designated as such by the Central Government based on factors like the volume and sensitivity of data processed, the risk to Data Principals' rights, and the potential impact on the sovereignty and integrity of India**. SDFs have additional obligations, including the mandatory appointment of a Data Protection Officer (DPO) based in India, the appointment of an independent data auditor, and the undertaking of periodic Data Protection Impact Assessments (DPIAs). The identification of SDFs signifies a tiered approach to compliance, with more stringent requirements for entities handling larger volumes of sensitive data or posing a higher risk to individuals' privacy.
Data Processor	This is **any person who processes personal data on behalf of a Data Fiduciary.** Data Processors act under the instructions of the Data Fiduciary and have certain obligations in handling personal data.

Consent Manager	This is a **registered entity that acts as a single point of contact for Data Principals to give, manage, review, and withdraw their consent**. Consent Managers aim to streamline the consent management process for Data Principals.
Personal data breach	This is **any unauthorized processing or accidental disclosure, acquisition, sharing, use, alteration, destruction, or loss of access to personal data that compromises its confidentiality, integrity, or availability.** Data Fiduciaries are obligated to give intimation of a personal data breach to the DPB and each affected Data Principal.

Obligations of Data Fiduciaries under the DPDP Act

Data Fiduciaries, entities that determine the purpose and means of processing personal data, bear several crucial obligations under the DPDP Act to ensure the protection of individuals' personal data and uphold their rights.

Lawful processing of personal data

Data Fiduciaries must ensure that personal data is processed only for a lawful purpose. Processing can occur based on the consent of the individual or for certain legitimate uses specified under the Act. Legitimate uses where consent may not be required include voluntary sharing of data by the individual, processing by the state for permits, licenses, benefits, and services, medical emergencies, and employment. The aim of the Act is to balance the rights of individuals with the necessity of processing data for lawful purposes.

Providing notice to the Data Principal

Before collecting personal data, Data Fiduciaries are obligated to provide a clear and easily understandable notice to the Data Principal. This notice should contain a description of the personal data sought to be collected and the purpose for the processing of such personal data. The notice should also inform Data Principals about the manner in which they can exercise their rights and make complaints. This notice and the request for consent should be accessible in English or any of the 22 languages included in the Eighth Schedule to the Constitution of India, at the option of the Data Principal.

Obtaining valid consent

When processing relies on consent, Data Fiduciaries must obtain explicit and informed consent from the Data Principal. The Act emphasizes the importance of informed consent, requiring Data Fiduciaries to provide clear and easily understandable information regarding the purpose, scope, and duration of data processing. For individuals below 18 years of age (children), consent must be provided by the parent or legal guardian, and it must be verifiable parental consent. There are also provisions for deemed consent under certain circumstances, such as legal or contractual obligations, vital or public interest, and legitimate interest.

Right to withdraw consent

Data Principals have the right to withdraw their consent at any point in time. Data Fiduciaries must respect this right and have mechanisms in place for Data Principals to easily withdraw their consent.

Cessation of processing upon withdrawal of consent

Once consent is withdrawn by the Data Principal, the Data Fiduciary must cease processing the personal data, unless there are legal obligations or legitimate interests to continue retention.

Implementing reasonable security safeguards

Data Fiduciaries are required to implement reasonable security safeguards to prevent data breaches and protect personal data from unauthorized access, disclosure, alteration, or destruction. This includes adopting robust security practices, conducting regular audits, and implementing necessary safeguards to mitigate risks. Failure to implement necessary information security measures to mitigate the risk of a personal data breach could result in significant fines.

Intimation of personal data breach

In the event of a personal data breach, Data Fiduciaries are obligated to inform the DPB and each affected Data Principal. This intimation should be made in the prescribed manner and likely within a specific timeframe, although the exact timeline might be further specified in rules. Failure to report personal data breaches can lead to penalties.

Erasure of personal data

Data Fiduciaries must erase personal data as soon as the purpose for which it was collected has been met or when the Data Principal withdraws consent, unless retention is necessary for legal purposes. The Act provides specific guidelines for the deletion and anonymization of personal data. However, storage limitation and the right to erasure may not apply to government entities.

Publishing contact information for grievance redressal

Data Fiduciaries are required to publish contact information for grievance redressal to enable Data Principals to raise concerns or complaints regarding the processing of their personal data.

Establishing grievance redressal mechanisms

Data Fiduciaries must establish mechanisms to address and resolve grievances raised by Data Principals in relation to the processing of their personal data. They are expected to respond to grievances within a reasonable timeframe, potentially within seven days or a shorter period as may be prescribed.

Obligations regarding children's and persons with disabilities' data

Processing the personal data of children (below 18 years) requires verifiable parental consent. The Act also prohibits tracking or behavioral monitoring of children and targeted advertising directed at children. While the definition includes persons with disabilities under the term Data Principal where a lawful guardian acts on their behalf, specific additional obligations beyond consent through a guardian are not explicitly detailed in the provided excerpts. However, the general principles of lawfulness, purpose limitation, and security would apply.

Additional obligations for SDFs

Entities identified as SDFs by the central government may be subject to additional obligations due to the volume and sensitivity of the personal data they process and the associated risks. These additional obligations may include:

- Appointment of a DPO based out of India.
- Appointment of an Independent Data Auditor.
- Conducting periodic DPIAs to identify and mitigate potential risks to the rights of Data Principals.

These obligations underscore the emphasis on accountability, transparency, and the empowerment of individuals regarding their personal data under the DPDP Act. Organizations need to be proactive in assessing their data processing activities and implementing necessary measures to ensure compliance with these requirements.

Rights of Data Principals under the DPDP Act

The DPDP Act grants several rights to individuals, referred to as Data Principals, empowering them with control over their personal data and promoting transparency and accountability in data processing. These rights include:

Rights	Explanation
Right to access information	Data principals have the **right to receive comprehensive information about the collection, processing, and purpose of collecting their personal data**. This includes the right to **know what personal data is being collected about them, the purpose for which it is being collected**, and **third parties with whom it is being shared.** Data Fiduciaries are obligated to **furnish clear and concise details concerning the utilization of individuals' data.** Furthermore, individuals have the right to **obtain information about the processing** of their personal data.
Right to correction and erasure	Data Principals retain the **prerogative to request rectification or have their personal data updated if found inaccurate or incomplete.** Data Fiduciaries are required to **promptly put into effect the necessary amendments** and inform relevant entities with whom the data has been shared. Additionally, individuals have the **right to request the deletion or erasure of their personal data under specific circumstances**. Data Fiduciaries must comply with such requests, ensuring that the data is no longer retained or utilized. This is also encompassed by the **right to be forgotten**, which allows individuals to request the erasure of their personal data under specific circumstances, requiring Data Fiduciaries to undertake necessary measures for permanent removal. The Digital Personal Data Protection Bill, 2023 explicitly grants the right to seek **correction and erasure of personal data**.

Right to nomination	The DPDP Act introduces a **unique right to nominate another person to exercise rights in the event of death or incapacity**. This ensures that even when a Data Principal is unable to manage their data rights, a designated individual can act on their behalf.
Right to grievance redressal	Data Principals have the **right to file a complaint with the DPB** if they believe that their personal data has been processed in a manner that is not in compliance with the DPDP Act. Data Fiduciaries are obligated to establish **processes to address Data Principals' redressal requests**. They are also required to publish contact information for grievance redressal. Data Fiduciaries are expected to **respond to the grievance of Data Principals within seven days or a shorter period that may be prescribed**. This right ensures a mechanism for individuals to seek resolution for issues related to the processing of their personal data.
Right to object	The sources indicate that individuals **possess the right to object to the processing of their personal data in particular situations.** Data Fiduciaries are obligated to respect these objections unless there exist legitimate grounds for data processing that outweigh the individual's interests.
Right to data portability	While earlier drafts and discussions of data protection legislation in India included the **right to data portability**, allowing individuals to acquire and transfer their personal data from one service provider to another, **the Digital Personal Data Protection Bill, 2023 does not grant the right to data portability to the Data Principal.**
Right to be forgotten	As mentioned under the right to correction and erasure, **the right to be forgotten,** allowing individuals to limit the disclosure of their personal data, is effectively covered by the right to request erasure under specific circumstances within the DPDP Act. The 2023 Bill grants the right to seek erasure.

In summary, the DPDP Act provides Data Principals with significant rights to control and manage their personal data, emphasizing transparency, accountability, and the ability to seek recourse in case of grievances. While some rights discussed in earlier stages, such as the explicit right to data portability, are not included in the final 2023 DPDP Act, the enacted legislation still provides a robust framework for protecting individual data privacy.

A CXO's guide to achieving DPDP compliance

A. Essential steps for DPDP Act compliance

For CXOs and business leaders, achieving compliance with the DPDP Act requires a strategic and systematic approach. The first essential step is to **determine the applicability of the Act to the organization's data processing activities.** This involves understanding whether the organization processes digital personal data within India or if its processing outside India relates to offering goods or services to individuals in India. Following this, organizations need to **build a comprehensive data inventory and data map** to understand what personal data they collect, where it is stored, how it is used, and with whom it is shared. This foundational step is crucial for identifying the scope of compliance efforts. **Implementing robust consent management mechanisms** is vital, ensuring that consent is obtained freely, specifically, informed, unconditionally, and unambiguously, and that individuals have the ability to withdraw their consent easily. Organizations must **also establish processes to enable Data Principal rights, such as the rights** to access, correction, erasure, nomination, and grievance redressal, ensuring timely and appropriate responses to such requests.

Adopting appropriate data protection measures and safeguards, including technical and organizational measures, is paramount to ensure the security and confidentiality of personal data and to prevent data breaches. It is also crucial for CXOs to understand the seriousness of DPDP Act enforcement and the potential penalties for non-compliance, which can be significant. If the **organization qualifies as a Significant Data Fiduciary, appointing a DPO based in India and conducting DPIAs for high-risk processing activities will be mandatory. Finally, employee training and awareness programs** are essential to ensure that all personnel handling personal data understand their responsibilities and the requirements of the DPDP Act. These steps provide a practical roadmap for organizations to navigate the complexities of DPDP Act compliance.

B. Developing a DPDP Act compliance checklist

To provide a more tangible guide for CXOs, a comprehensive DPDP Act compliance checklist can be a aluable tool. The following table synthesizes key requirements from the Act and related analyses:

Compliance area	Checklist item	Status
Applicability	Determine if the organization processes digital personal data within India.	☐ Yes ☐ No
	Determine if the organization processes digital personal data outside India related to offering goods or services to individuals in India.	☐ Yes ☐ No

Policies and procedures	Establish a data usage and protection policy covering data protection principles, data subject rights, consent management, data sharing, breach notifications, etc.	☐ Yes ☐ No
	Establish a data processing and retention policy defining authorized processing and data retention periods.	☐ Yes ☐ No
Employee training	Conduct regular training sessions for employees on DPDP Act requirements and data protection policies.	☐ Yes ☐ No
	Implement a process for new joiners to receive mandatory training on data privacy and security.	☐ Yes ☐ No
Data inventory and mapping	Map all personal data collected, processed, and stored.	☐ Yes ☐ No
	Document how personal data is collected, used, stored, and accessed.	☐ Yes ☐ No
	Identify data owners and access permissions for personal data.	☐ Yes ☐ No
Consent management	Implement mechanisms to obtain free, specific, informed, unconditional, and unambiguous consent.	☐ Yes ☐ No
	Provide clear privacy notices in English and other specified Indian languages.	☐ Yes ☐ No
	Ensure a process for Data Principals to easily withdraw consent.	☐ Yes ☐ No
	Maintain records of consent obtained.	☐ Yes ☐ No
Data security	Implement reasonable security safeguards to prevent data breaches.	☐ Yes ☐ No
	Encrypt personal data at rest and in transit.	☐ Yes ☐ No
	Implement access controls and regularly monitor access logs.	☐ Yes ☐ No
Data breach	Establish procedures for identifying, reporting, and documenting personal data breaches.	☐ Yes ☐ No
	Ensure a process for notifying the DPB and affected Data Principals of a breach.	☐ Yes ☐ No

Data Principal rights	Establish procedures for Data Principals to exercise their rights (i.e., access, correction, erasure, nomination, grievance redressal).	☐ Yes ☐ No
	Ensure timely responses to Data Principal requests.	☐ Yes ☐ No
SDF (If applicable)	Appoint a DPO based in India.	☐ Yes ☐ No
	Appoint an independent data auditor.	☐ Yes ☐ No
	Conduct periodic DPIAs.	☐ Yes ☐ No
Data retention and erasure	Establish data retention schedules based on the purpose of processing.	☐ Yes ☐ No
	Implement procedures for securely erasing personal data when no longer needed or upon withdrawal of consent.	☐ Yes ☐ No

This checklist provides a structured framework for organizations to assess their readiness for DPDP Act compliance and track their progress.

C. Understanding the role of Data Protection Impact Assessments (DPIAs)

DPIAs are a critical component of a robust data privacy framework, particularly under the DPDP Act. A DPIA is a **process designed to identify and assess potential risks to the privacy of individuals** associated with the processing of their personal data. While the DPDP Act explicitly mandates DPIAs for SDFs, it is considered a best practice for any organization undertaking processing activities that could pose a high risk to the rights and freedoms of Data Principals. High-risk processing might include the use of new technologies, large-scale processing of sensitive data, or activities that could lead to discrimination or significant harm if data is compromised.

The process of conducting a DPIA typically involves several key steps.

1. First, the **organization needs to describe the nature, scope, context, and purposes of the processing operation.** This includes detailing what personal data will be processed, how it will be processed, the duration of processing, and who will have access to it.

2. Next, a **thorough assessment of the necessity and proportionality of the processing in relation to the purposes is required.** This step ensures that the data collected is adequate, relevant, and not excessive for the intended purpose, aligning with the principle of data minimization.

3. The core of the DPIA **involves identifying and assessing the risks to Data Principals, considering the likelihood and severity of potential impacts** such as loss of confidentiality, integrity, or availability of data, or potential harm to individuals.

4. Finally, the organization must **identify measures to address the risks, demonstrating how it will mitigate, transfer, or accept the identified risks to ensure an appropriate level of data protection.** Conducting DPIAs helps organizations proactively identify and address privacy risks, ensuring that data protection is integrated into the design and operation of their processing systems and practices.

D. Managing consent and Data Principal rights

Effective management of consent is central to DPDP compliance, as consent serves as a primary lawful basis for processing personal data.

1. The DPDP Act sets a high standard for valid consent, requiring it to be **free, specific, informed, unconditional, and unambiguous,** given through a clear affirmative action.

2. Organizations must **ensure they provide clear and accessible privacy notices to Data Principals** before seeking their consent, explaining the categories of personal data to be collected, the specific purposes for processing, the process for exercising their rights, the procedure to revoke consent, and how to file complaints.

3. **Obtaining blanket consent for multiple purposes is not permissible**; consent must be specific to each purpose of processing.

4. Furthermore, the process for **withdrawing consent must be as easy as giving it**. Organizations need to implement mechanisms to record and manage consent, including the date and time of consent, the specific purposes for which consent was given, and any subsequent withdrawals.

5. A consent-first approach necessitates a **re-evaluation of existing data collection and processing practices** to ensure they align with these stringent requirements.

6. Operationalizing the rights of Data Principals, such as the rights to access, correction, and erasure, requires organizations to **establish clear procedures and ensure timely responses.**

7. For access requests, organizations need to **verify the identity of the Data Principal and provide them with a summary of their personal data being processed**, the processing activities undertaken, and the identities of any Data Fiduciaries or Processors with whom the data has been shared.

8. For correction requests, **organizations must allow Data Principals to request the rectification of inaccurate or misleading personal data**, the completion of incomplete data, and the updating of their data.

9. Handling **erasure requests involves deleting the personal data of the Data Principal when they withdraw consent, unless retention is necessary for compliance with other laws.**

Organizations **should have dedicated channels and trained personnel to handle these requests efficiently and within the timelines** that may be specified in the forthcoming rules. Implementing robust identity verification processes and maintaining accurate records of data processing activities are crucial for effectively managing Data Principal rights requests.

Leveraging ManageEngine AD360 for DPDP Act compliance

ManageEngine AD360 is a unified identity and access management (IAM) solution designed to simplify complex IT challenges, including meeting various requirements of the DPDP Act. It achieves this by integrating multiple components into a single platform for managing, auditing, securing, and reporting on the IT infrastructure, including Windows Active Directory, Microsoft 365, Exchange Servers, and cloud applications.

Here's an overview of AD360's **key features** and how it helps enterprises comply with the DPDP Act:

DPDP Act requirement	Feature/ component	Description	How it addresses DPDP Act compliance
Data accuracy			
Maintaining accuracy of data. Automated processes reduce manual errors in data management within Active Directory.	Management and automation capabilities - **ADManager Plus**	**ADManager Plus**, one of the components of AD360, provides management, reporting, automation, and workflow capabilities for Active Directory. This includes ensuring accurate user information during provisioning and updates.	By providing tools for managing and automating user account creation and modifications in Active Directory, AD360 can help **maintain the accuracy of data stored** within these systems. Also, the automated processes help reduce manual errors effectively.

Data security			
Preventing data breaches, ensuring confidentiality and integrity significantly enhances security and reduces the risk of unauthorized access to data.	MFA -**ADSelfService Plus**	**ADSelfService Plus,** another AD360 component, offers MFA to secure access to critical resources and apps. This includes various authenticators and adaptive MFA based on context.	Implementing MFA significantly enhances security by adding an **extra layer of verification,** thus protecting data from unauthorized access, a key requirement of the DPDP Act. Adaptive MFA further strengthens security based on risk factors.
Preventing unauthorized access, ensuring confidentiality and integrity. Limits data access based on necessity, minimizing the risk of unauthorized disclosure.	**Role-Based Access Control (RBAC)**	AD360 provides **RBAC,** allowing non-admin users to perform IT tasks with help desk delegation and custom roles. Granular delegation based on OUs, groups, etc., ensures controlled access.	RBAC helps **limit access to data to only those with a legitimate need,** minimizing the risk of unauthorized disclosure or breaches, which aligns with the DPDP Act's emphasis on data security and confidentiality.
Preventing data breaches, detecting security incidents. Continuous monitoring helps in timely intervention against unauthorized access attempts that could lead to data breaches.	Real-time auditing and alerting - **ADAudit Plus**	**ADAudit Plus**, an AD360 component, performs real-time change auditing and alerting for Active Directory. This includes monitoring user activities and detecting suspicious logons and file access.	Continuous monitoring and alerting capabilities help in the **early detection of security incidents and unauthorized access attempts** that could lead to personal data breaches, allowing for timely intervention as mandated by the DPDP Act.
Accountability			
Demonstrating accountability, facilitating audit trails. Maintaining logs of data processing activities provides evidence of security measures and data handling practices.	Comprehensive audit reports - **ADAudit Plus, Exchange Reporter Plus, M365 Manager Plus**	AD360 integrates reporting from components like **ADAudit Plus, Exchange Reporter Plus**, and **M365 Manager Plus.** These provide detailed audit reports on Active Directory, Exchange, and Microsoft 365 activities that includes user management actions like creation, deletion, password resets, and permission changes, along with details on who did what, when, and from where.	Maintaining **detailed audit logs of activities related to data processing** across various systems helps **organizations demonstrate** accountability, a key principle of the DPDP Act. These reports can be used for investigations and compliance audits.

Leveraging ManageEngine Log360 for DPDP Act compliance

ManageEngine Log360 is a unified security information and event management (SIEM) solution that integrates data loss prevention (DLP) and cloud access security broker (CASB) capabilities. Its primary function is to help organizations proactively detect, prioritize, investigate, and respond to security threats while also aiding in meeting compliance requirements like the DPDP Act.

Here's an overview of Log360's **key features** and how it helps you comply with the DPDP Act:

DPDP Act requirement	Feature/ component	Description	How it addresses DPDP Act compliance
Accountability			
Accountability of Data Fiduciaries maintaining audit trails for demonstrating compliance and investigating incidents, aiding in understanding the **purpose of processing** and data collected.	SIEM - **Centralized log management**	Enables the collection, parsing, analysis, storage, and searching of log data from diverse sources across the IT infrastructure, including network devices, servers, applications, and cloud platforms.	Provides a **central repository of security-related data for audit trails and investigation of potential breaches.** Helps in **demonstrating accountability.**
Facilitates **demonstrating accountability** and adherence to the DPDP Act by providing **audit-ready reports** on security measures and data processing activities.	Compliance - **Comprehensive compliance reporting**	Offers 30+ prebuilt audit templates for popular mandates and regulatory standards including those related to data security (e.g., ISO 27001, PCI DSS). For optimal fine-tuning to meet organization specific reporting and new regulations, the core modules can be tailored and custom compliance reports can be constructed through customization wizard, which includes correlation rule building, report generation, alert criteria mapping, anomaly modeling, and audit report generation.	Aids in **demonstrating compliance** with data protection regulations by providing evidence of security measures and data handling practices.

Directly supports the **accountability of Data Fiduciaries** by maintaining a **historical record of data access and processing,** crucial for audits and investigations.	Audit a accountability - **Detailed audit trails**	Maintains comprehensive audit trails of data access and processing activities across the IT infrastructure, including Active Directory, network devices, applications, and cloud platforms. Provides a historical record of actions taken within the system.	Essential for **demonstrating accountability** for the processing of personal data and for investigating potential security incidents or breaches.
Data security			
Preventing data breaches, ensuring **data security,** upholding the **integrity and confidentiality of personal data,** and facilitating timely action upon suspicious activity that could lead to a breach.	**Integrated DLP**	Identifies unusual file or data accesses, cut down malicious communication to command and control (C&C) servers, and prevent data from being exfiltrated.	Aids in the early **detection of potential data breaches** and **unauthorized access to data**, aligning with the principle of **integrity and confidentiality.**
Enhancing data security by leveraging threat intelligence to prevent breaches and unauthorized access to personal data.	SIEM - **Advanced threat analytics**	Leverages threat intelligence feeds and dark web monitoring to enhance the accuracy of threat detection by providing up-to-date information on known malicious entities and emerging threats.	Improves the ability to **detect and prevent security incidents that could compromise personal data.**
Ensuring data security, maintaining the **integrity and confidentiality of personal data**, and preventing **unauthorized disclosure.**	**Integrated DLP**	Helps to discover, classify, and protect sensitive data, including personal data, within the network to prevent unauthorized access and exfiltration. Includes features for data discovery, classification, and monitoring.	Directly contributes to the **integrity and confidentiality of personal data by preventing data leakage and unauthorized handling.**
Securing personal data in cloud environments, ensuring **data security** and preventing **unauthorized access** in line with the obligations of Data Fiduciaries.	**Integrated CASB**	Provides security monitoring and governance for cloud environments, ensuring that personal data stored and processed in the cloud is protected and compliant with security policies.	Extends **security controls and visibility to cloud resources where personal data might reside.**

Data breach			
Efficiently identifying and responding to potential breaches, contributing to the **duty to prevent data breaches** by reducing noise and highlighting genuine threats.	**Attack detection - Comprehensive threat detection and data protection**	It integrates: 1) Multi-layered threat detection (i.e., rule-based correlation, ML-driven UEBA, and MITRE ATT&CK framework integration); 2) Data protection; 3) Compliance management; 4) Incident response. It covers on-premises, cloud, and hybrid environments with features like shadow IT monitoring, web content filtering, and remote workforce security.	Provides end-to-end protection of data by preventing breaches, ensuring security via continuous monitoring of data access and modifications, and maintaining integrity through file tracking and change alerts.
Detecting insider threats and compromised accounts, contributing to the **duty to prevent data breaches** and **ensure data security.**	SIEM - **UEBA**	Uses ML to establish baselines of normal activity for users and entities, and then identifies anomalous behavior that could indicate a security threat, insider risk, or compromised accounts.	Helps in detecting unusual activities that could signal a **personal data breach or unauthorized access.**
Efficient incident response to potential data breaches, aiding in fulfilling the **duty to report data breaches** to the DPB and affected Data Principals in a timely manner.	**Security Orchestration, Automation, and Response (SOAR)**	Automates incident management workflows, streamlining the process of alert resolution, threat neutralization, and response to security incidents.	**Facilitates a faster and more efficient response to potential personal data breaches**, which is **crucial for meeting notification requirements.**
Maintaining the accuracy and **integrity of personal data**, detecting **unauthorized changes,** which aligns with the duties of Data Fiduciaries.	DLP - **File integrity monitoring**	Monitors critical files for any unauthorized changes, alerting administrators to potential tampering with data, including personal data.	Helps maintain the **integrity of personal data by detecting unauthorized modifications** and preserving confidentiality with content-aware DLP and exfiltration prevention.

Enables **timely reporting of data breaches** by providing **early warnings** of suspicious activities, crucial for meeting regulatory requirements for notification.	Incident handling - **Real-time alerts and notifications**	Provides timely alerts when suspicious activities or potential security incidents are detected, enabling security teams to respond quickly.	Facilitates a **rapid response to potential personal data breaches,** which is critical for minimizing impact and meeting notification timelines.
Assists in fulfilling the **duty to report data breaches** by providing a centralized platform for managing incidents and documenting the necessary details for reporting.	Incident handling - **Incident management console**	Offers a centralized platform for managing, tracking, and documenting security incidents, including data breaches.	Supports the process of **investigating and documenting personal data breaches**, which is necessary for notification to the DPB and affected Data Principals.
Contributes to the **duty to prevent data breaches** by providing a **centralized view of security events,** enabling quicker detection of threats and unauthorized actions.	Audit and accountability - **Activity dashboard**	Provides a centralized view of key security events and activities, allowing administrators to quickly identify any suspicious or unauthorized actions.	Helps in the **rapid identification of potentially malicious activities that could lead to a data breach.**

Conclusion and recommendations

Compliance with the DPDP Act is not merely a legal obligation but a fundamental aspect of building trust and ensuring the responsible handling of personal data in India. ManageEngine AD360 and Log360 offer significant value to organizations striving to meet the requirements of this Act.

AD360 strengthens identity and access controls, enforces security policies, and maintains crucial audit trails, addressing key principles like integrity and confidentiality. Log360 provides real-time security monitoring, advanced threat detection, robust data breach identification and notification capabilities, comprehensive audit logging, and integrated data loss prevention, further bolstering an organization's security posture and compliance efforts.

To effectively leverage these solutions for DPDP Act compliance, organizations should:

- Conduct a thorough assessment of their data processing activities to fully understand the scope and applicability of the DPDP Act.
- Implement a comprehensive data inventory and mapping exercise to identify all personal data being processed.
- Utilize AD360 to implement strong MFA, enforce RBAC, and regularly review audit logs to ensure only authorized personnel have access to personal data.
- Deploy Log360 to continuously monitor their IT environment for security threats, detect potential data breaches, and establish clear procedures for reporting and responding to incidents in a timely manner.
- Stay informed about any further rules, regulations, and guidelines issued by the Indian government and the DPB to adapt their compliance strategies accordingly.
- Invest in comprehensive employee training programs to raise awareness about the DPDP Act and ensure that all personnel understand their roles and responsibilities in protecting personal data.
- Consider seeking expert legal and data privacy advice to ensure a holistic and compliant approach to the DPDP Act.

By strategically implementing and utilizing AD360 and Log360, organizations can significantly enhance their ability to comply with the DPDP Act, safeguard the personal data of individuals, and build a culture of privacy and security.

Our Products

Log360 | ADManager Plus | ADAudit Plus | ADSelfService Plus
Exchange Reporter Plus | RecoveryManager Plus

About AD360

ManageEngine AD360 is a unified identity platform that seamlessly connects people, technology and experiences while giving enterprises full visibility and control over their identity infrastructure. It offers automated life cycle management; secure SSO; adaptive MFA; and risk-based governance, auditing, compliance and identity analytics—all from a single, intuitive console. With extensive out-of-the-box integrations and support for custom connectors, AD360 easily integrates into existing IT ecosystems to enhance security and streamline identity operations. Trusted by leading enterprises across healthcare, finance, education, and government, AD360 simplifies identity management, fortifies security and ensures compliance with evolving regulatory standards.

For more information, please visit www.manageengine.com/active-directory-360/.

$ Get Quote Download

Our Products

AD360 | ADAudit Plus | EventLog Analyzer | DataSecurity Plus
Exchange Reporter Plus | M365 Manager Plus

About Log360

Log360 is a unified SIEM solution with integrated DLP and CASB capabilities that detects, prioritizes, investigates and responds to security threats. Vigil IQ, the solution's TDIR module, combines threat intelligence, an analytical Incident Workbench, ML-based anomaly detection and rule-based attack detection techniques to detect sophisticated attacks, and it offers an incident management console for effectively remediating detected threats. Log360 provides holistic security visibility across on-premises, cloud and hybrid networks with its intuitive and advanced security analytics and monitoring capabilities.

For more information about Log360, visit manageengine.com/log-management/ and follow the LinkedIn page for regular updates.

$ Get Quote Download